When do cyber operations amount to use of force and armed attack, and what response will they justify?

Candidate number: 723
Submission deadline: April 25, 12 p.m.
Number of words: 17808
# Table of contents

1 INTRODUCTION .............................................................................................................. 1  
1.1 Introduction to the issue ............................................................................................. 1  
1.2 Terminology ................................................................................................................ 2  
1.3 Methodology ............................................................................................................... 4  
1.3.1 Treaties ................................................................................................................. 6  
1.3.2 International Customary Law .................................................................................. 7  
1.3.3 General principles of law ....................................................................................... 7  
1.3.4 Subsidiary means for the determination of rules of law ....................................... 8  
1.3.4.1 Judicial decisions ............................................................................................... 8  
1.3.4.2 The use of published scholars .......................................................................... 8  
1.3.4.3 The International Law Commission .................................................................. 9  
1.3.4.4 The Tallinn Manual ........................................................................................... 10  
1.4 The research question and scope of the thesis ......................................................... 10

2 HOW CYBER OPERATIONS WORK OUT ...................................................................... 12  
2.1 The Cyber Kill Chain ................................................................................................. 12  
2.2 Categories of weapons for attacking computers ....................................................... 14  
2.3 Examples of cyber attacks ......................................................................................... 16  
2.3.1 The Slammer worm (2003) .................................................................................. 16  
2.3.2 Estonia (2007) ..................................................................................................... 17  
2.3.3 Stuxnet (2010) ..................................................................................................... 17

3 WHAT CONSTITUTES "USE OF FORCE"? ................................................................. 19  
3.1 Article 2(4) in the UN Charter and the concept of "use of force" .............................. 19  
3.2 International customary law ...................................................................................... 21  
3.3 Leading approaches to use of force .......................................................................... 22  
3.3.1 Scale and effects ................................................................................................... 23  
3.3.2 When does a cyber operation rise to the level of a "use of force" under article 2(4)? ................................................................................................................................. 26

4 WHAT CONSTITUTES AN "ARMED ATTACK"? ...................................................... 30  
4.1 The gap between "use of force" and "armed attack" ................................................. 30  
4.2 The concept of "armed attack" in the cyber context .................................................. 32  
4.3 The element of national critical infrastructure ....................................................... 33

5 THE SCOPE FOR RESPONDING TO CYBER OPERATIONS .................................. 36
5.1 Evidential requirements and attribution ................................................................. 36
  5.1.1 The general rule of evidentiary under international law ................................. 36
  5.1.2 The specific considerations that apply to cyber operations ............................ 36
  5.1.3 Attribution ........................................................................................................ 38
    5.1.3.1 The attribution of acts by non-state actors to a state .............................. 41
  5.2 Countermeasures .................................................................................................. 41
  5.3 Self-defense .......................................................................................................... 44
    5.3.1 The UN Charter article 51 ............................................................................. 44
    5.3.2 The right to self-defense in international customary law ............................... 45
    5.3.3 The criteria for self-defense .......................................................................... 48
      5.3.3.1 The principle of proportionality ............................................................... 48
      5.3.3.2 The principle of necessity ........................................................................ 49
      5.3.3.3 The principle of immediacy ................................................................. 50
  6 CONCLUSIONS ........................................................................................................ 52
  7 TABLE OF REFERENCE ......................................................................................... 53
1 Introduction

1.1 Introduction to the issue

The examination of this topic is more than anything concerned with principles of law than actual practice, since no force has been acted out through cyberspace in a way that is generally acknowledged. However, the examples of cyber operations known to the public are providing us with some kind of warning: the worst-case scenarios explained by scholars could actually happen, based on the potential previous incidents have illustrated.

The concepts of use of force, armed attack and the following responses to them are important in the context of cyber operations for several reasons. There is some discourse around whether the existing legal realm is applicable to the matter at all. If it is, the question is how the relevant rules and customary law should be interpreted. If it is not applicable, however, the international community is left with a gap in the regulation of force, and needs to act in order to achieve an agreement on how attacks through cyberspace should be regulated. The strategy in the Chinese Publication “Unrestricted Warfare” describes catastrophic use of common hacker tools like this:

[i]f the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent’s computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatch network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots and a political crisis.¹

Such a scenario leaves us with questions like these:

- Is an attack on a foreign state’s computers or network an illegal use of force under the UN Charter or customary international law?

- Does such an attack trigger a nation’s right to self-defense or other responses?
- Who did it and how can the attack be attributed to a state or a non-state actor? Which difficulties rise when applying the rules of attribution of the cyber domain?

These are some of the questions this thesis will attempt to answer.

The United States declared in its view to the UN Secretary General that the ambiguities of cyberspace "simply reflect the challenges…that already exists in many contexts".\(^2\)

### 1.2 Terminology

This chapter will present and explain the terminology used in this thesis. Due to the complexity of the terms, an explanation will ease further reading and clarify any uncertainties. Some of the terms are used interchangeably by some scholars, and consistently by others.

Typically, cyber incidents fall within one of four categories: crime, terrorism, espionage, and war – each with its own unique characteristics and applicable legal instruments.\(^3\) A fifth category is emerging and is involving government use of cyber weapons against political opponents.\(^4\) The latter and the categories crime, terrorism, espionage will not be discussed in this paper.

Cyber attacks fall within the broader category of what is traditionally known as “information operations”.\(^5\) Information operations are the

“…integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security in

\(^2\) UN Doc A/66/152, 15 July 2011, p. 18.


concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own”.

According to the 2006 United States Military Strategy for Cyberspace Operations, “computer network operations” (CNO), include computer network attacks (CNA), computer network defense (CND) and "related computer network exploitation" (CNE). Although they are often labeled in the media as "cyber attacks", CNE operations are different as they focus on intelligence collection and observation rather than network disruption and can be preliminary to an attack. CNE can be used for propaganda purposes or be aimed at stealing sensitive information from websites or computers. Espionage and intelligence collection is, however, not prohibited by international law, although it is usually criminalized at the domestic level. CNE will not be further discussed, as is falls outside the scope of this thesis.

**Computer network attacks**

An early definition of computer network attacks, but one still in use by The U.S Department of Defense, is:

"[A]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves".

**Cyber attack**

A cyber attack involves the deliberate, unauthorized insertion of a cyber weapon into software-operated machines in order to accomplish the tasks the programmer engineered the code to perform. Note that this definition is broader than some definitions of "cyber attack" in order to capture the broadest scope of activities for analysis. Other definitions of the term restrict "cyber attacks" to destructive activities and exclude actions that exploit cyber

---

technologies for intelligence purposes.\textsuperscript{13} This thesis will focus on the former option; cyber attacks with potential for destructive effects.

**Cyber weapon**

A "cyber weapon" can be defined as:

"[A] packet of binary computer code engineered to accomplish surreptitious tasks through software-operated machines, such as computers, servers, routers, mobile phones or industrial equipment."\textsuperscript{14}

**Cyber warfare**

The last term to be described here is the one that could be characterized as military operations. This paradigm consists of the following: (a) warfare proper (the conduct of military operations within the framework of armed conflict), and (b) "operations other than war", which means operations related to conflict, but outside the framework of armed conflict.\textsuperscript{15}

The International Committee of the Red Cross (ICRC) understands the term as operations against a computer system through a data stream, when used as means and methods of warfare in the context of an armed conflict, as defined under International Humanitarian Law (IHL).\textsuperscript{16} As the term is related to \textit{jus in bello}, it will not be further discussed.

In the following, the terms “cyber attacks”, “cyber operations” and "computer network attacks" will be used interchangeably.

**1.3 Methodology**

States have not directly regulated the use of cyber operations in a binding treaty nor otherwise, even though Russia has been advocating such agreements.\textsuperscript{17} Nor have they dealt with this sophisticated technology long enough for state practice to be established.

\textsuperscript{13} Roscini, M (2010), p. 92, see note 11.
\textsuperscript{16} International Committee of the Red Cross, 31st International Conference of the Red Cross and Red Crescent, \textit{"International Law and the Challenges of Contemporary Armed Conflicts"}, Report 31IC/11/5.1.2, October 2011, p. 39.
In the following sections, I will elaborate on the primary sources of international law before turning to the secondary means of interpretation.

International law requires a different approach than domestic law, as international law does not have a universally established methodical structure.\(^{18}\) Neither is there a common legislature between states nor a body able to create laws internationally binding upon everyone, nor a proper system of courts with compulsory or comprehensive jurisdiction to interpret and extend the law.\(^{19}\) Shaw describes this problem as follows:

"One of the major problems of international law is to determine when and how to incorporate new standards of behavior and new realities of life into the already existing framework, so that, on the one hand, the law remains relevant and, on the other hand, the system itself is not too vigorously disrupted".\(^{20}\)

Although limited to the sources of law that the ICJ must apply, the provisions of Article 38 is often put forward as the sources of international law.\(^{21}\) According to Article 38(1), the Court shall apply:

a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
b) international custom, as evidence of a general practice accepted as law;
c) the general principles of law recognized by civilized nations;
d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

The Article is not intended to create a hierarchy among the sources as such, but it is acknowledged that subparagraphs a) and b) are the most important ones: we can explain the priority of a) by the fact that it refers to a source of obligation (a treaty) which will ordinary

\(^{19}\) Shaw, (2014), p. 49
prevail as being more specific than custom and general principles. The exception to this horizontal view is where peremptory rules – *jus cogens* – prohibits derogation, thus creating a vertical dimension. *Jus cogens* reflect fundamental values that are "so essential for the protection of fundamental interests of the international community that [their] breach [was] recognized as a crime by that community as a whole" (emphasis added). Examples of such breaches are slavery, genocide and apartheid.

1.3.1 Treaties

Treaties are known by many different names, but all the terms have one thing in common: they refer to the creation of written agreements whereby the states participating bind themselves legally to act in a particular way or to set up particular relations between themselves. The obligatory nature of treaties is founded upon the customary international principle that agreements are binding (*pacta sunt servanda*). Treaties only create law between the states who are parties to it. Treaties may not impose obligations on third states, unless the third state give consent to assuming the obligations or existing rights laid down in the treaty. In short, nothing can be done without or against the will of a sovereign state. This is one of the most prominent features of international law, which also complicates the drafting of treaties and other obligations, due to the fact that consensus is necessary. Furthermore, the states may make reservations if they find some of the clauses in the treaty too onerous, but nonetheless want to enter into the treaty.

Different rules regarding the interpretation of treaties have been put forward over the years, and include the textual approach, the restrictive approach, and the teleological approach. Article 31 in the Vienna Convention of the Law of Treaties (VCLT) emphasizes the intention of the parties as expressed in the text, as well at the wording in context with the object and purpose as the best guide to the correct interpretation. The International Court of Justice

---

(ICJ) found that "an international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation". The concept of dynamic, or evolving interpretation, which is implemented in Article 31(3)(b) of VCLT, was employed by the Court in a subsequent ruling, where it held that:

"Where parties have used generic terms in a treaty, the parties necessarily having been aware that the meaning of the terms was likely to evolve over time, and where the treaty has been entered for a very long period or is "of continuing duration", the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning".

In accordance with the Court’s ruling, the terms “use of force” and “armed attack” must be understood in accordance with today’s dependency on technology. The discussion of whether a cyber attack can constitute use of force and an armed attack will follow below in chapters 3 and 4.

1.3.2 International Customary Law

The rules created by means of treaties, either bilateral or multilateral, are not stronger than, or superior to, customary or general rules. Article 38 refers to "international custom, as evidence of a general practice accepted as law". In order to determine the existence of customary law, two questions have to be answered: 1) is it a general practice; and 2) is it recognized as international law? Judge Read has described customary law as "the generalization of the practice of states".

1.3.3 General principles of law

Every now and then, an international court may be confronted with a case where there is no law covering that exact point, neither parliamentary statute nor judicial precedent. If such a situation occurs, the judge will proceed to deduce a relevant rule, either by analogy from

---

35 Fisheries (UK v Norway), ICJ Reports 1951, para. 191 (Judge Read).
existing rules or directly from general principles that guide the legal system such as justice, equity or considerations of public policy. This way, the court will be guided by “general principles of law recognized by civilized nations” and therefore will choose, edit and adopt from other legal system, in order to arrive at a reasonable solution.

1.3.4 Subsidiary means for the determination of rules of law

The words of Article 38(1)(d) are to be utilized as subsidiary sources for the determination and interpretation of legal rules, rather than an actual source of law.

1.3.4.1 Judicial decisions

Judicial judgments are important in different ways. They are, in many instances, regarded as evidence of the law. This is shown in the way the ICJ strive to follow its previous judgments, former jurisprudence will has important consequences in following cases.

In a case, the Court may create law in the process of interpretation, such as by defining the wording in a treaty, or for example, set out criteria to determine whether an act constitute a breach of an obligation.

In addition to The International Court of Justice, the phrase “judicial decisions” encompasses international arbitrary awards and the rulings of national courts.

1.3.4.2 The use of published scholars

Due to the fact that there are very few hard sources of law on the subject of cyber operations, the arguments presented in this thesis are, to a large extent, derived from published scholars. The phrase “most highly qualified” is not given a restrictive effect, although the authority of the author naturally affects the weight given. One problem with scholarly writing is that subjective factors affect any publication, and can reflect either national or other prejudices.

39 Brownlie, (2012), p. 50
44 Brownlie, (2012), p. 43.
Books and academic articles are important as a way of arranging and putting into focus the structure and form of international law, and clarify the nature, history and practice of legal rules, as well as pointing out difficulties and defects that exist within the system and make suggestions for the future. The latter is especially prominent in the context of cyber attacks, as the legal instruments under *jus ad bellum* do not consider this context. Then, as noted during the work with this thesis, there is the work of academics that fuel the discussion around the applicability of the rules and the practical side of them.

Even though publicists enjoy wide use, the ICJ seems to make few or no references to such writings, with the exception of some dissenting opinions.

1.3.4.3 *The International Law Commission*

The work by the International Law Commission (ILC) is analogous to the writings of publicists. Their work includes, inter alia, the Draft Articles on State Responsibility, commentaries, reports and secretary memoranda.

The ILC was created as a subsidiary organ under the UN General Assembly under Article 13(1)(a) of the Charter, and turned out to be more successful in terms of codification than its equivalent bodies under the Hague Conventions and The League of Nations. The purpose of the Commission was to promote the progressive development of international law and its codification, and their work has resulted in, inter alia, The Vienna Convention on the Law of Treaties and The Vienna Convention on Diplomatic Relations.

The relevant work by the ILC in this thesis is The Draft Articles on State Responsibility; which international tribunals and courts have relied on as an authoritative statement on the Law of State Responsibility. In 1997, President Schwebel of the ICJ stated in a speech to UN General Assembly that:

"[T]he fact that just as the judgments and opinions of the Court has influenced the work of the International Law Commission, so the work of the Commission may influence that of the Court."

48 Brownlie, (2012), p. 44.
In 2009, a group of 20 renowned Western law scholars and practitioners met at the NATO Cooperative Cyber Centre of Excellence in Tallinn, Estonia to discuss whether a manual on the applicable law to cyber warfare should be written. The result, The Tallinn Manual, examines the international law governing “cyber warfare”, and includes cyber-to-cyber operations only.\textsuperscript{50}

Even though the manual has been supported by most states, Russia has rejected it due to lack of legitimacy. The Manual does not have more authority than other scholar writings, but since it is the first serious attempt to address the law applicable to cyber operations, it has been cited over and over again by scholars and officials. Therefore, it seems to be the best liable source on the prevailing view among most western scholars.

1.4 The research question and scope of the thesis

In the following discussions, I presuppose that the \textit{jus ad bellum} paradigm is applicable to cyber operations.\textsuperscript{51}

The research question is the following: Under \textit{jus ad bellum}, when do cyber operations amount to use of force and armed attack, and what response will they justify? The scope is limited to the use of cyber force by one state against another state, within the \textit{jus ad bellum} paradigm, which is the body of international law that governs a State’s resort to force as an instrument of its national policy.\textsuperscript{52} Cyber activities that occur below the level of use of force, like cyber crimes, cyber terrorism or cyber attacks committed by individuals or "hacktivist" groups such as Anonymous or will not be addressed here. Nor will it deal with questions

\textsuperscript{50} Schmitt, M. (n.d.), \textit{Tallinn manual on the international law applicable to cyber warfare}, Cambridge University Press, p. 4-5. (hereinafter The Tallinn Manual)

\textsuperscript{51} The applicability of \textit{jus ad bellum} to cyber operations has been emphasized by several states and international organizations, i.e. the United Nations. Based on the views submitted by the UN member states, the Reports of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security set up by the UN General Assembly found that: "[I]nternational law, and in particular the Charter to the United Nations, is applicable and is essential to maintaining peace and stability and promoting and open, secure and accessible ICT [Information and Communications Technologies] environment." See Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013, available at: www.un.org/en/ga/search/view_doc.asp?symbol=A/68/98 , para. 19. (Last accessed 4 March 2016)

\textsuperscript{52} The Tallinn Manual, p. 42.
regarding human rights issues. Due to the word limit, anticipatory self-defense and the exercise of self-defense will not be discussed.

In the following, I will first explain how a cyber operation is carried out, based on the Cyber Kill Chain framework, and present some examples that will be used in the discussions below. Then I will analyze the existing framework for "use of force" and "armed attack" and apply these to the cyber context. Furthermore, the problems related to evidential requirements and attribution will be addressed, followed by the criteria for countermeasures and self-defense as responses to "use of force" and "armed attack".
2 How cyber operations work out

2.1 The Cyber Kill Chain

The purpose of this part is to explain how a cyber operation is carried out. Most state cyber agencies, like the Norwegian Cyber Defense\(^{53}\), use the Cyber Kill Chain framework, a model for identification and prevention of cyber intrusions, developed by the American company Lockheed Martin. A kill chain is a systematic process to target an adversary to create desired effects.\(^{54}\) From a defensive point of view, the objective is to understand and handle the intrusion in such a way to give the defender an advantage over its opponent. In many situations this can be stopping the action, but other times it could be observe and learn what the attacker is doing. Analyzing an attack according to the Kill Chain model enables the defender to make this choice.

The Cyber Kill Chain by Lockheed Martin consists of the seven steps illustrated by the figure below. The kill chain illustrates the seven steps the attacker must complete in order to launch a cyber operation. Because all the seven steps have to be completed, adversaries stopped by the cyber defense at any stage breaks the chain of attack.

The model operates with separate approaches within each step for the adversary and the defender. Below I will focus on the steps taken from the attacker’s point of view.

Figure 2: The cyber kill chain.\(^{55}\)

---

\(^{53}\) [Link to article](http://www.tu.no/artikler/er-det-is-eller-russland-slik-over-fremtidens-norske-cybersoldater/276500)


The seven steps that have to be completed are:\textsuperscript{56}

1) Reconnaissance

The first step is all about identifying the target, and includes both traditional intelligence operations, and scanning and technical examination of the networks. The adversaries are still in their planning phase, and are doing research in order to understand which targets that will enable them to meet their objectives. The choice of target can be triggered by different situations. For example, the Norwegian Defense Armies became the target of a cyber attack after they decided to participate in the bombing of Libya in 2011.\textsuperscript{57}

2) Weaponization

After the target of the operation has been selected, the preparation and staging phase starts. This includes the creation of the malware.\textsuperscript{58} The generation of malware, such as a virus\textsuperscript{59}, can be done either by hand or by using automated tools, depending on the sophistication, skill and resources the attacker possesses.

3) Delivery

This step marks the launching of the operation, where the malware created in step 2 are directed towards the target. The delivery can be done in different ways, such as malicious e-mails, malware on USB-sticks or through web pages. The uses of USB-sticks are necessary if the attacker wants to access a closed system without connection to the Internet, and the malware therefore has to be inserted manually to a computer connected to the closed system.

4) Exploitation

This phase describes the situation where the intruder gains access to the victim. After the delivery is completed, the malware will exploit known or unknown (zero days)
vulnerabilities in the network or on the computer to engage access. The weak spot can be found in either hardware, software, or be a result of human vulnerability. What happens when the victim either has clicked on a malicious link or attachment (typically sent via e-mail), a program will start to run on the computer. Then, the program has to take advantage of vulnerability on the computer. For example, if the victim opens a malicious pdf-file, the malware has to exploit vulnerability in the pdf reader program.

5) Installation
Typically, the malware installs a persistent backdoor or implant to maintain access for an extended period of time. The malicious pdf that was opened will now make itself persistent by hiding files on the computer and change settings so the files will start running every time the computer is starting. The attackers challenge is to make sure the files are hidden well enough.

6) Command and control (C2C)
The installed malware opens a command channel to enable them to remotely control the victim. This means that a two-way communication is created\(^6\), via channels like the web and e-mail protocols.

7) Action on objectives
If the attacker reaches this step, the mission goal is achieved. From here, the intruder have a limitless arsenal of options, and what happens next depends on who is on the keyboard. Examples of such action is stealing files, monitor keystrokes for usernames and password and encrypt files for ransom.

2.2 Categories of weapons for attacking computers

Cyber attacks can originate from several different sources, depending on the perpetrator and the intension of the attack. Michael Vatis, former head of the Institute for Security Technology Studies at Dartmouth College, has identified four sources categories of threats: terrorists, nation-states, terrorist sympathizers and thrill seekers.\(^6\) In this thesis, the category of nation-states will be discussed. States will, most likely, have access to the greatest capabilities and resources, both in terms of technology, economy and qualified personnel.

---
\(^6\) Also known as a backdoor/trapdoor; an undocumented way of gaining access to a program, online service or an entire computer system. Diniss, (2012), p. 293.

However, not all states have this competence, making private hackers on contract a useful resource. The attribution of acts committed by such non-state actors will be discussed under section 5.1.3.1. Furthermore, several states have over the last years developed their own military cyber security units and have included cyber incidents in their national military manuals. This must be seen as a signal that the states are taking the threats from the cyber domain seriously, and that they are aware of the capabilities and possibilities that can be carried out through cyber technology.

Judge Advocate in the US Army, Sean Condron, argues that nation-states, despite their capabilities and awareness of the issue, most likely will refrain from the use of computer network attacks, unless it is precursor to a military response, due to the potential severity of their response.\textsuperscript{62} Seen in context with the fact that states have territory, property and citizens to protect, there is a chance that all of this could be jeopardized if the state were to attempt a major cyber attack.\textsuperscript{63} On the other hand, states would probably refrain from the use of conventional weapons for the same reasons.

There are three main categories of weapons for attacking computers, based on the type of cyber weapon used.\textsuperscript{64}

1) A physical attack using conventional weapons directed against a computer facility or its transmission lines,

2) An electronic attack (EA) using electromagnetic energy to insert a stream of malicious code directly into enemies transmissions, or using an electromagnetic pulse of directed energy to overload computer circuitry; and,

3) A computer network attack (CNA), usually involves inserting a stream of malicious code into enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. Other forms of CNA are enabled when the attacker uses stolen information to enter a restricted computer system.

It is important to note that over time, technology might evolve and create new ways to attack and disturb computer systems and the functions that they control. Generally, a computer network attack is an attempt to disrupt the integrity or authenticity of data, in most cases through interfering with the code that controls data. The attacked data are corrupted by sending malicious signals, such as a virus or a Trojan Horse, through a network to infect computers.

A different possibility is the use of stolen passwords of credentials to gain unauthorized access to either encrypted or legitimate systems. It does not seem to matter whether the network is open or restricted in some way. In order to perform a successful cyber attack, the attacked computer is required to have some type of system flaw, such as lack of antivirus protection or a malfunction in the system configuration. The malicious codes take advantage of this weakness in order to exploit and infect the system.

2.3 Examples of cyber attacks

2.3.1 The Slammer worm (2003)

One of the most prominent factors to a CNA is that they spread quickly. In 2003, a computer worm known as “Slammer” attacked Microsoft’s database software and spread through the Internet over the space of one weekend. The Slammer worm spread to infect more than 90 percent of vulnerable computers within 10 minutes after it was released. The worm took advantage of a known vulnerability in Microsoft’s SQL Server, even though Microsoft had released a patch who would repair the weakness almost a year earlier. The worm caused considerable harm through network outages and unpredictable consequences such as cancelled airline flights, ATM failures and interference with elections. Although Microsoft denied that serious damage did occur, a report published by the Centre for Strategic and

---

68 A worm is a subclass of virus which does not require human intervention to spread from host to host. Worms take advantage of file or information features on the computer system to allow it to travel unaided. Dinniss, (2012) p. 296.
International Studies (CSIS) stated that "if this could happen to Microsoft, then no company is safe".\(^7\)

2.3.2 Estonia (2007)

Estonia, one of the most wired countries in the world, was attacked April 26, 2007. The attacks brought the banking system, many governmental services and much of the media to a halt.\(^7\) The distributed denial of service attack (DDoS)\(^7\) followed the Estonian government's decision to move a Soviet-era statue to another location, which caused outrage among Russians in both Estonia and Russia.\(^6\) The attacks were mainly, although not exclusively, conducted from outside of Estonia were carried out by so-called "patriot hackers" from 178 different countries.\(^7\) At first, the attacks were "simple, ineptly coordinated and easily mitigated".\(^7\) However, the attacks quickly became far more organized and sophisticated.\(^7\) In particular, large botnets were used. A botnet is a collection of high jacked computers that can be used without the knowledge of the owner.\(^8\) In the Estonia case, approximately 85 000 botnets were requesting information from Estonian Internet Web Pages.\(^1\) Although the Russian government denied responsibility for the attacks and no attribution has been made, Estonia maintained that Russia was responsible.\(^2\)

2.3.3 Stuxnet (2010)

Using four unknown vulnerabilities in the computer network system\(^8\), the Stuxnet attack in 2010 was allegedly designed to force a change in the uranium centrifuges´ rotor speed at the


\(^7\) Denial of service attacks is a type of attack that is designed to bring a system to its knees by feeding it with useless traffic; the sum effect is that legitimate users are denied access. Dinniss, (2012), p. 294.


\(^7\) Dinniss, (2012), p. 15.


\(^8\) Russel, (2012), p. 211

\(^1\) Russel, (2012), p. 211


\(^8\) Probably one of the noted vulnerabilities described in the section about CNA above.
Natanz uranium enrichment plant in Iran, causing inductive excessive vibrations or distortions that would damage the centrifuges. The change of rotor speed made the centrifuges inoperable, and, reportedly, Iran had to replace thousands of components after the attack. The International Atomic Energy Agency (IAEA) reported that Iran stopped feeding uranium into thousands of centrifuges at Natanz, a claim denied by the Iranian authorities. The perpetrators are widely acknowledged as Israel and The United States, although not confirmed.

One of the most prominent features of the Stuxnet worm was its precision. The precision of the worm meant that collateral damage beyond the targeted centrifuges did not occur. However, it seems unclear whether this was the intention of the perpetrators or not.

It has been argued that under international law, the attacks constituted both an illegal use of force and an armed attack against Iran. The alleged perpetrator states, however, and Iran, have not characterized the incident as a use of force, an armed attack nor an illegal act of aggression. Others argue that the Stuxnet episode was a covert cyber operation that amounts, at most, to an illegal intervention in the domestic affairs of Iran.

Stuxnet, at least, demonstrated that states are capable to design cyber weapons to be precise and cause little to no collateral damage. However, this does not mean that all cyber attacks launched in the future will have such indiscriminate features. Most likely, Stuxnet only demonstrates a small part of the possible outcomes that may result from a cyber attack.

3 What constitutes "use of force"?

3.1 Article 2(4) in the UN Charter and the concept of "use of force"

Article 2(4) in the UN Charter famously states that:

\[\text{[a]ll Members shall refrain in their international relations from the threat of use of force against the territorial sovereignty or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations}.\]

The predominant significance of the article has been emphasized by authors, who have labeled it "the corner stone of peace in the Charter"\(^{92}\), and "the heart of The United Nations Charter".\(^{93}\)

Under the terms of Article 2(4), the distinction between war and other acts of force has disappeared.\(^{94}\) The prohibition covers every unlawful threat or use of force under whatever reason guise they figure.\(^{95}\) The use of force in general is prohibited, rather than only war.\(^{96}\) It is important to determine whether a use of force is present because the victim state may have a broader range of options than if the incident of attack does not constitute a use of force.\(^{97}\)

There is no official definition of, or criteria for, "threat of use of force" or "use of force".\(^{98}\) Attempts to apply the contextual and literal criteria in order to establish the meaning of "force" have been proven inconclusive. According to Black's Law Dictionary, "force" means "power, violence, or pressure against a person or thing".\(^{99}\) This means that the force could be broad enough to cover not just armed force, but also political and economic coercion. However, these kinds of coercion are not a part of the prohibition in Article 2(4).

\(^{92}\) Waldock. C. H. M., The Regulation of the Use of Force by Individual States in International Law, Rec de Cours 81 (1952-II), 451-417, p. 492
\(^{93}\) Henkin, L., The Reports Of The Death of Article 2(4) are Greatly Exaggerated, AJIL 65 (1971), 544-548. p. 544
\(^{97}\) Jensen, (2002), p. 214
\(^{98}\) The Tallinn Manual, p. 46.
A closer examination of the norm in reference to its context within the UN Charter, to its spirit and purpose as well as drafting history, leads to the conclusion that "force", in the meaning of Article 2(4), means "armed force" only.\textsuperscript{100} It follows from the wording and structure of The Friendly Relations Declaration that Article 2(4) is to be interpreted as embodying a narrow meaning of force, confined to military or armed force.\textsuperscript{101}

The question, then, is if and when a cyber operation reaches the level of a use of armed force.\textsuperscript{102} According to Black’s Law Dictionary, "armed" means "[e]quipped with a weapon" or "[i]nvolved in the use of a weapon".\textsuperscript{103} A weapon is "[a]n instrument used or designed to be used to injure or kill someone".\textsuperscript{104} Roscini points out that almost every object can be used as a weapon, if the intention of the holder is hostile.\textsuperscript{105} The use of the term "weaponized" about a malicious code indicates that the code itself has characteristics that are intended to serve as a tool for disruption or destruction, just like a kinetic weapon.

Furthermore, in its Advisory Opinion on the Legality of the Use of Nuclear Weapons, the ICJ stated that Articles 2(4), 51 and 41 "do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed."\textsuperscript{106}

This leads to the conclusion that if a cyber operation amounts to a use of force, it is irrelevant for the classification that the force was acted out through cyber means. There is then, based on the statements from The Court, no reason why weapons should necessarily have explosive effects or be created for explosive purposes only.\textsuperscript{107} The use of biological and chemical weapons, both dual-used non-kinetic weapons, would undoubtedly be treated as a use of force by the victim state.\textsuperscript{108} In addition to this, the ICJ implicitly recognized that the use of non-

\textsuperscript{105} Roscini, Marco, (2010), p. 106.
\textsuperscript{107} Roscini, (2010), p. 106.
\textsuperscript{108} Roscini, (2010), p. 106
kinetic force can lead to a violation of Article 2(4) when it qualified the arming and training of the contras by the United Stated as a threat or use of force against Nicaragua. 109

3.2 International customary law

The recognition of the prohibition of use of force as international customary law is not disputed today. In the Nicaragua Case, the ICJ adopted this view as well. As the Merits of the case will be a central part of the discussions below, a summary of the facts in the case will be given here.

In 1979, the right-wing Somoza Government was overthrown by revolution by the left-wing Sandinista Government. Two years after the revolution, President of the United States, Ronald Reagan, terminated the American economic aid to Nicaragua on the ground that it had aided guerrillas fighting against the El Salvador Government, which enjoyed good relations with the United States. 110 Nicaragua had allowed the Soviet Union arms to pass through their ports and territory on the way to El Salvador, which created a problematic situation in the already tense Cold War.

In the following case at the International Court of Justice, Nicaragua claimed that the United States had used direct armed force against their territory by placing mines in Nicaraguan internal and territorial waters, caused damage to ports, oil installations and a naval base, and, assisted the Contras, the guerrillas fighting against the Sandinista Government. 111

Furthermore, Nicaragua claimed that the United States had breached the 1956 US-Nicaragua Treaty of Friendship, Commerce and Navigation. 112

The Court ruled, inter alia, that the United States had violated the prohibition of use of force under customary law and the obligation not to intervene in Nicaragua`s internal affairs and to not violates their sovereignty. 113

112 Nicaragua, para. 23.
113 Nicaragua, para. 292.
The Nicaragua judgment applied the international customary law prohibition on the resort to force, stating that the United States had violated its “obligations under customary international not to use force against another State.”

3.3 Leading approaches to use of force

Whether a cyber operation falls within the scope of Article 2(4) or not, will ultimately depend on how the nature of a cyber attack is understood. Three main approaches have been developed, and there is some discourse around their applicability, seen in context with the traditional understanding of use of force. The approaches are also applicable under the armed attack discussion, but will be introduced here and referred to below.

The instrument-based approach is focusing on the means to commit an act, for i.e. weapons, and is what traditionally distinguishes armed force from economic and political coercion. This approach harmonizes poorly with cyber operation, due to focus on physical means, and under this approach, a malicious code would never, and no matter what consequences it produces, be a use of force. It follows by a textual reading of the UN Charter, that the more analogues a new weapon is to conventional weapons, the more likely its operation will constitute use of force, or an armed attack.

The target-based approach argues that cyber attack must target national critical infrastructure (NCI), in order to constitute use of force. It doesn’t seem to matter if the attack produces any effects, as long as it is directed against NCI. There are two problems, however. First, the approach is too broad, and would lead to the result that a cyber operation qualifies as use of force if it only cause inconvenience or merely aim to collect information. Second, there is not a generally accepted definition of critical national infrastructure, which may lead to different practice depending on the notion within different countries. Critical infrastructure will be further addressed below.

114 Nicaragua, para. 292, (4), (6).
Both the instrument- and the target-based approach have the clear advantage that an incident would be easy categorized. But they are too narrow to catch the complexity of cyber operations, and on the other hand they are over inclusive.

The consequence or effect-based approach has received most support of the three, and recognize that states are more concerned with the consequences of a cyber operation than the weapon or the nature of the target.\textsuperscript{119} The United States has noted that the international communities will more likely focus on the consequences of a cyber attack than on its mechanism.\textsuperscript{120}

The approach is intended to identify cyber operations that are analogues to other non-kinetic or kinetic actions that the international community would describe as uses of force.\textsuperscript{121} However, this view does not take into account that the dependency of modern societies on computers, computer systems and networks has made it possible to incapacitate physical infrastructures without destroying them.\textsuperscript{122} Furthermore, consequences are hard to measure objectively, and more gray area cases will occur.

3.3.1 Scale and effects

In this section I will discuss when a cyber attack will constitute use of force under the consequence-based approach.

The phrase “scale and effects” is sourced from the \textit{Nicaragua} Judgment,\textsuperscript{123} where The Court drew a distinction between an armed attack and a "mere frontier incident".\textsuperscript{124}

According to rule 11 in The Tallinn Manual, a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.\textsuperscript{125} This notion, however, raises a number of new questions. How do one measure the effect of a cyber attack, and is it possible to compare the effects with the ones from a physical attack? Since the Charter does not provide any criteria by which to determine when an act

\begin{flushright}
\end{flushright}
amounts to a use of force, the question remains open. The authors of the Tallinn Manual (The International Group of Experts) took notice of the Nicaragua judgment.\textsuperscript{126} In that case, the International Court of Justice stated that "scale and effects" are to be considered when determining whether particular actions amount to an "armed attack".\textsuperscript{127} The International Group of Experts found the focus on scale and effects to be an equally useful approach when distinguishing acts that qualify as uses of force from those that do not.\textsuperscript{128} This means that "scale and effects" is a pedagogic term that captures the qualitative and quantitative factors to be analyzed when to determine whether a cyber operation qualifies as a use of force.

In the article \textit{Cyber attacks, self-defense and the problem of attribution}, Professor Arva Constantinou has tried to specify the scale and effects standard by arguing that an armed attack is:

\begin{quote}
"An act or the beginning of a series of acts of armed force of considerable magnitude and intensity (ie. scale) which have as their consequences (ie effects) the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority, ie. its political independence, as well as damage to, or deprivation of its physical element namely, its territory".\textsuperscript{129}
\end{quote}

Constantinou includes both the scale and effects of the use of force that determine the occurrence of an armed attack.\textsuperscript{130} For example, a massive DoS attack (like the one that occurred in Estonia) involving millions of botnets that only disrupts the national critical infrastructure for a limited amount of time will be significant enough with regard to its scale, but its effects are not.\textsuperscript{131}

The destructive objective of a cyber attack does often not center on the direct damage or disruption on the computer or the computer itself, but on the indirect effects from the cyber attack. The effects will usually materialize on the systems or devices controlled by the

\textsuperscript{126} The Tallinn Manual, p. 45.
\textsuperscript{127} Nicaragua, para. 195.
\textsuperscript{128} The Tallinn Manual p. 45-46.
\textsuperscript{130} Tsagourias N (2012), p. 231.
\textsuperscript{131} Roscini (2014), p. 73.
targeted computer or on the human decision maker that depends on information that the targeted computer or computer system contains or processes.\textsuperscript{132} Reports on the Stuxnet attack often refers to the effects on the nuclear facilities, and not necessary the attack on the computer system controlling the centrifuges. This may indicate that even though cyber attacks are targeting computers and computer systems, it is the visible effects and damages that catch our attention. This is confirmed by the fact that many attacks will not be discovered before they cause damage or disruption outside of the computer system.

According to Reese Nguyen, the thing that matters are not so much that the effects are indirect, but more importantly, these effects are removed from the actors that caused them.\textsuperscript{133} The operator of the cyber operation has, like the pilot of a drone, removed themselves from the battlefield and the targets they are planning to strike against. Then again, the predicted use of large scale cyber attacks, will not be directed against soldiers, but larger infrastructure facilities that, in serious situation, will have impact on more than soldiers, but also civilians.

As explained above, cyber attacks can result in multiple effects. However, the idea of armed force having direct effect leading to instant damage or injures, should be reconsidered in the cyber context. In his book \textit{Cyber Operations and the Use of Force in International law}, Professor Marco Roscini argues for a breakdown of the effects into three types: primary, secondary and tertiary effects. The primary effects are those on the attacked computer, computer system or network, such as the deletion, corruption, or alteration of data or software.\textsuperscript{134} He also mentions the disruption through a DoS attack or other types of cyber attacks. The secondary effects are those on the infrastructure operated by the attacked computer or computer network, i.e. its total or partial destruction or incapacitation.\textsuperscript{135} Tertiary effects are those on the persons or property affected by the destruction or incapacitation of the attacked computer or network, i.e. the electricity produced by power plant targeted by a cyber attack.\textsuperscript{136} Based on the levels described above, Roscini claims that that physical damage to property or injury or loss of life can never be a primary effect of a cyber attack. Damage to property can only be a secondary of tertiary effect, while injury or loss of life only can be a

\textsuperscript{132} Nguyen, (2013), p. 1098.
\textsuperscript{133} Nguyen, (2013), p. 1099.
\textsuperscript{134} Roscini, (2014), p. 52.
\textsuperscript{135} Roscini, (2014), p. 52.
\textsuperscript{136} Roscini, (2014), pp. 52-53.
tertiary effect. By dividing the effects in such way, the unique features of how a cyber attack work out are highlighted.

Based on the arguments above, the most prominent factor to be considered when determining if a cyber operation is a use of force are the effects of the attack.

3.3.2 When does a cyber operation rise to the level of a "use of force" under article 2(4)?

In order to answer this, the overall question that can be asked is: have enough of the qualities of a use of force been identified to characterize the information operation as a use of force?137

Since the consequence-approach itself does not provide much guiding on how to consider cyber operations, the authors of the Tallinn Manual138 have proposed eight factors that states are likely to consider and place great weight on when deciding whether a cyber operation amount to a use of force.139 The factors are: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality. These factors are not exhaustive, nor legal criteria.140 Depending on the circumstances, the State may look to others, such as the prevailing political environment, the identity of the hacker, any records of cyber operations by the hacker, and the nature of the target.141 The factors operate in concert, which means that several of the factors can be present, with different significance depending on the attack. The criteria are useful for parsing out many of the characteristics that identify armed force: the greater the severity, immediacy and directness, the more likely the act is an armed force.142

I will not discuss all of them here, but I will accentuate the ones that are highlighted in the academic discussion. The factors will also be relevant when discussing whether cyber operations constitute an armed attack.

139 The factors are: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality. The Tallinn Manual, p. 48-51.
The identification of the action, meaning the source of the subsequent effects is crucial, and represents a problem under several of the factors. Identification in this context must not be confused with attribution of the attacker, which will be discussed under section 5.1.3.

Severity has been labeled the most important factor, and includes the level of harm or damage that was caused to individuals and property, with an eye towards the scale, scope, and duration of consequences. This can be seen as analogous to conventional weapons. A cyber operation causing effects similar to those caused by a kinetic weapon, are more likely to be considered a use of force.

One could argue that there is a minimum threshold of severity that the destructive consequences of a cyber attack needs to reach in order to be a violation of Article 2(4) and not only the principle of non-intervention. For instance, former Legal Advisor of the Department of State, Harold Koh, appears to distinguish between injury/death of persons on one hand and damage to property on the other when he argues in a speech that it is “cyber activities that proximately result in death, injury or significant destruction” that would be considered a use of force. In the same speech, Koh proposed factors to be considered when assessing whether an attack is a use of force, including: the context of the event, the actor perpetrating the action, the target and location, effects and intent.

The immediacy of the attack is a way to describe the duration of the force. If the attack materialize in seconds to minutes and catch the state off guard (not giving it a chance to avoid or neutralize it), it is more likely that the cyber operation will be characterized as a use of force, than if it takes weeks or months. On the other hand, the malware causing the effects can be complex and produce different effects over time, depending on if it has reproduced itself and infected other computers or systems. The total scope of such malware is hard to identity, and therefore it may be hard to determine the effects caused by it. Immediacy and directness are closely related; the more directed a cyber operation is towards the target, the more immediate will the attack act on the target.

The directness of the attack points to the causation between the initial act and resulting consequences; the more direct, the more likely it should constitute a use of force.\textsuperscript{147}

However, \textit{indirectness} is one typical characteristic of computer network attacks, as a large number of possible attacks will manipulate one system to achieve a knock-on effect from something else.\textsuperscript{148} Examples of such indirect attacks include manipulation of GSP satellite systems to send an opposing missile off target, disabling air traffic control systems, or manipulating of hospital blood type data resulting in the wrong blood type being given to the wrong soldier.\textsuperscript{149} With reference to the secondary and tertiary effects described by Roscini, these as all actions that require further action by a second actor or objective to achieve the desired result. These indirect features where also described in Nicaragua, where the training of the guerilla constituted use of force. Most likely, according to Dinniss, the example of the hospital records would not be considered as use of force, because the second actor had no intention to cause damage but is used as an involuntary actor.\textsuperscript{150}

Based on the levels of effect and the factors provided in the Tallinn Manual described above, it seems clearer why the consequence approach has the most support among scholars. If the traditional notion of force as a force resulting in damage, injury or loss of life as a primary effect (like the ones of a kinetic weapon), a cyber attack will never be included under Article 2(4). Based on the knowledge available on the effects that a cyber attack may result in, that is not a satisfactory interpretation. As noted by Waxman;

"\textit{modern society`s heavy reliance on interconnected information systems means that the indirect and secondary effects of cyber-attacks may be much more consequential than the direct and immediate ones}."\textsuperscript{151}

If there is a cause and effect chain between the computer network attack and following violent consequences, it is irrelevant whether they were produced by traditional or cyber weapons.\textsuperscript{152}

\textsuperscript{147} Dev, (2015), p. 391  
\textsuperscript{149} Dinniss, (2012), p. 66.  
\textsuperscript{150} Dinniss, (2012), p. 66.  
Waxman’s prediction is, however, not necessary a problem for the application of the *jus ad bellum* rules: in the Nicaragua judgment, the ICJ expressly recognized that intervention that uses armed force could occur either directly or indirectly. Therefore, the nexus between an act of a state and a destructive effect on the victim state will be of critical importance.\textsuperscript{153}

So far, as described above, it is uncontested that a cyber attack resulting in or most likely resulting in physical damage to property, loss of life or injury to persons would be a violation of the prohibition under Article 2(4). On the other hand, no cyber attack has been reported to cause such consequences. If one excludes the explosion of a Soviet gas pipeline in Siberia in 1982, apparently caused by a logic bomb inserted in the computer controlled system by the US CIA,\textsuperscript{154} the first known use of a malicious worm to cause damage to property is Stuxnet. The causation of physical damage, however, does not necessarily require acting on the software: Roscini argues that it may be sufficient to gain access to the computer system and delete or alter, for example, transport or medical data for trains to collide, airplanes to crash, or for patients to receive the wrong medical treatment.\textsuperscript{155}

Commonly cited examples of cyber activity that would constitute a use of force include, for example: operations that trigger a nuclear meltdown, operations that open a dam over a populated area and operations that disable air traffic control resulting in airplane crashes.\textsuperscript{156}

Koh also stated that:

"Only a moment’s reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force".\textsuperscript{157}

\textsuperscript{153}Dinniss, (2012) p. 66.
\textsuperscript{154}Rid, Thomas, (2013), *Cyber war will not take place*, Journal of Strategic Studies, Vol. 35, Iss. 1, 2012
\textsuperscript{155}Roscini, (2010), p. 53.
\textsuperscript{156}Koh, (2012), p. 4.
\textsuperscript{157}Koh, (2012), p. 4.
4 What constitutes an "armed attack"?

4.1 The gap between "use of force" and "armed attack"

According to Article 51 of the UN Charter, "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."

When compared to the wording of the prohibition in article 2(4), the terminology in the exception in article 51 suggests a different threshold for "use of force" and "armed attack".¹⁵⁸ The gap is not necessary wide, as the ICJ held in the Oil Platforms Case where it did not exclude "the possibility that the mining of a single military vessel might be sufficient to bring into play the inherent right of self-defense".¹⁵⁹ Dinstein has suggested that the gap between "use of force" and "armed attack", if it exists, has been exaggerated by the ICJ and is in reality very narrow, and he states that it is only use of force that does not result in victims or destruction of property that falls short of an armed attack.¹⁶⁰

The scope of article 2(4) is wider than that of article 51, because it does not only prohibit armed force, but also unarmed and indirect modes of means of force, in addition to the threat of force.¹⁶¹ In other words, not every kind of use of force is an armed attack.¹⁶² This discrepancy is both necessary and intended, as use of force below the threshold of an armed attack is not of sufficient gravity to justify a response on derogation from the Charter regime of collective enforcement, prohibition of unilateral force and peaceful settlement of disputes.¹⁶³ The restriction in Article 51 expresses the purpose in the Charter to prevent unnecessary escalation of interstate force, and by doing so, it puts the common interest of preserving international peace security before the interest of individual states to protect national sovereignty.¹⁶⁴ Only when the prohibited use of unlawful force rises to an armed attack can states use forcible measures for its defense. However, this authority is limited in

¹⁵⁸ Melzer, p. 11.
¹⁵⁹ Case Concerning Oil Platforms, (2003), (Iran v. United States), Merits, ICJ Reports 2003, para 72. (hereinafter Oil Platforms)
¹⁶¹ Melzer, p. 11.
¹⁶² Nicaragua, para 191.
¹⁶⁴ Melzer, p. 12.
two ways. First, the State acting in self-defense must observe the principles of proportionality and necessity, and second, it has to report immediately to the Security Council the measures taken, and it has to disconnect them as soon as the latter itself has taken the necessary measures for the maintaining of international peace. The criteria of proportionality and necessity will be discussed below.

Equivalent to The armed attack threshold does not only apply to an operation using traditional means, but also to operations using cyber means, to the extent that it amounts to a use of force under Article 2(4). ICJ supports this view in the Advisory Opinion on Nuclear Weapons, where The Court is stating that the choice of means of an attack is irrelevant to the issue of whether an operation qualifies as an armed attack. By saying this, the Court confirms the view that the choice of means or weapons is irrelevant, first stated in the Nicaragua case. Dinstein seems to agree, and marks on this subject that an armed attack can be carried out with “conventional, unconventional, primitive or sophisticated, ordnance”. Dinstein argues that a computer network attacks causing severe damage to property or human fatalities as a result; it would qualify as an armed attack.

Based on these statements, it seems reasonable to conclude that the choice of cyber weapons for use in an attack, does not affect the applicability of the traditional "armed attack" threshold, as the consequences will be decisive.

Randelzhofer argues in the UN Charter Commentary that a cyber attack in principle can carry out an armed attack. He claims that a cyber attack in order to raise to an armed attack, it must produce substantial and immediate effects, comparable to the effects produced by a conventional attack. In order to determine whether the attacks reaches the necessary destructive effects, one must take into account the immediate inhibitive effects (meaning that the destruction isn’t quickly repairable) on the ability of the state to act, or on the elementary living conditions of the population. This means that an individual consideration has to be made for each attack, taking into account the importance and the character of the protected

---

166 Advisory Opinion, para 30.
property for the affected state. Having in mind that states have different levels of dependence to technology, there is possible for an attacker to reach a diverse specter of infrastructure and facilities, depending on how wired the country is. The most dependent states will then be the ones most vulnerable to cyber operations. The most prominent example is the attack on Estonia, as described above. Since several of the most elementary governmental, economical and media facilities was so dependent on the Internet, it made them an easy target for the hackers, leaving the country in a state of isolation and standstill.

4.2 The concept of "armed attack" in the cyber context

In the Nicaragua Judgment, the ICJ simply remarked that “[t]here appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks”.\textsuperscript{172} This may be correct with regard to the use of conventional weapons, but in the cyber context, this is far from undisputed. Then again, the cyber threat and its possibilities were still in a fetal state at this point. By stating the concept of armed attack like this, the ICJ failed to provide a more precise definition in Nicaragua, and have not provided one later.

From a textual perspective, the notion of “armed attack” simply implies the use of a weapon. Just as in the case of use of force, the ICJ Advisory Opinion on Nuclear weapons will be applicable here, making the choice of weapon irrelevant. While cyber operations do not depend on the availability of traditional, conventional weapons, they cannot be carried out without the infrastructure making up cyberspace, thus raising the question of its qualification as a weapon.\textsuperscript{173} On this note, Karl Zemanek convincingly states in the book “Armed Attack”:

“[I]t is neither the designation of a device, nor its normal use, which make it a weapon, but the intent which it is used and the effect. The use of any device or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore de deemed to fulfill the conditions of an ´armed attack´.”\textsuperscript{174}

\textsuperscript{172} Nicaragua, para. 195.
This conclusion was supported by the Security Council`s reaffirmation of the right to self-
defense in relation to the 9/11 attacks on the United States, where hijacked planes where 
recognized as weapons.\textsuperscript{175}

The Tallinn Manual states in its Rule 13 that:

"A State that is the target of a cyber operation that rises to the level of an armed 
attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes 
an armed attack depends on its scale and effects."\textsuperscript{176}

The International Group of Expert concluded that some cyber operations might be sufficiently 
grave to warrant classifying them as “armed attacks” in the meaning of The UN Charter.\textsuperscript{177}
Furthermore, The Group of Experts concluded that Stuxnet was a use of force, and according 
to some of the experts, even an armed attack.\textsuperscript{178}

\textbf{4.3 The element of national critical infrastructure}

In his book "War, Aggression and Self-defense", Dinstein has suggested some examples of 
cyber attacks that would be serious enough to amount to an armed attack:

\begin{quote}
“Fatalities causes by the loss of computer-controlled life-support systems; an 
extensive power grid outage (electricity blackout) creating considerable deleterious 
repercussions; a shutdown of computers controlling waterworks and dams, generating 
thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through 
misinformation fed into aircraft computers)’ and “the wanton instigation of a core-meltdown 
of a reactor in a nuclear power plant, leading to the release of radioactive materials that can 
result in countless casualties if the neighboring areas are densely populated.”\textsuperscript{179}
\end{quote}

What these examples have in common is that they are all attacks on national critical 
infrastructure. As already noted, it is not only cyber attacks causing physical damage that

\textsuperscript{175} See SC Res 1368 (12 September 2001) and SC Res 1373 (28 September 2001).
\textsuperscript{176} The Tallinn Manual, p. 54.
\textsuperscript{177} The Tallinn Manual, p. 54
\textsuperscript{178} The Tallinn Manual, p. 58.
could amount to a use of force or an armed attack, but also those that severely incapacitate critical infrastructure so to affect state security. This view is in accordance with the target-based approach, as described above. However, it is reasonably to expect that a severe attack on critical infrastructure, also may lead to injury on persons or property? The United States seems be addressing this issue by focusing their approach on cyber security around critical infrastructure, as seen in their 2001 USA PATRIOT Act, where critical infrastructure is defined as

"[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economical security, national public health or safety, or any combination of those matters".

Furthermore on this note, the National Strategy to Secure Cyberspace defines critical infrastructure to include networks vital to the nation. Other critical infrastructures listed include the following sectors: agriculture, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, and postal and shipping.\textsuperscript{180} Both private and governmental agencies operate critical infrastructures. It goes without saying that such critical infrastructure as noted above is essential for the survival of the nation, and that in modern times, computer networks are the nerve center of the functioning of these. According to The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets in the United States, private industries operate approximately 85 percent of the nation’s critical infrastructure, and that the private sector largely unable to adequately protect these computer systems and networks against military and terrorist threats.\textsuperscript{181} However, military networks are also vulnerable because they depend extensively on civilian networks for connectivity and transferability of information.

Another question to be discussed is if the attack must be directed against a certain computer or computer system in order to be considered as an armed attack on the state. In an article published in the British newspaper The Guardian, Misha Glenny claimed that an attack on the


\textsuperscript{181} The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, p. 8 at: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (last accessed 24 April 24, 2016)
American company Google would be an attack on the US critical infrastructure.\textsuperscript{182} In a traditional military context, there would be no need to distinguish between military and civilian objects, as the state where the target is located would be entitled to self-defense because its territorial integrity has been violated.\textsuperscript{183} Hence, Dinstein argues that there is no need to come to a different conclusion on cyber operations because a traditional armed attack against a civilian facility on the territory of the target state would amount to an armed attack even if no members of the armed forces is injured or military property damaged:

"Even if the CNA impinges upon a civilian computer system which has no nexus to the military establishment (like a private hospital or institution), a devastating impact would vouchsafe the classification of the act as an armed attack."\textsuperscript{184}

\textsuperscript{182} Glenny, Misha. (2010), In America’s new cyber war Google is on the frontline, The Guardian, 18 January 2010, \url{http://www.theguardian.com/commentisfree/2010/jan/18/america-cyberwar-google-china-computer} (last accessed 19 April 19, 2016)

\textsuperscript{183} Roscini (2014), p. 76.

\textsuperscript{184} Dinstein, (2002), p. 106
5 The scope for responding to cyber operations

5.1 Evidential requirements and attribution

The justification of response measures, like countermeasures to a use of force or self-defense to an armed attack, requires that the victim state can provide evidence for the wrongful act. Evidence is required to prove both the objective and the subjective elements.

5.1.1 The general rule of evidentiary under international law

International law does not provide a general standard of evidence of all internationally wrongful acts, and the international courts and tribunals have determined their own standards in each case, and not always in a consistent matter. As the ICJ held in the Nicaragua Judgement,

“within the limits of its Statute and Rules...[The Court] has freedom in estimating the value of the various elements of evidence.”

However, the application of an evidentiary requirement to a legal question has two aspects. First, one has to substantiate the factual claims made by the parties, and second; one has to determine which of the parties who carry the burden of the proof. The burden of proof is “the obligation on a party to show that they have sufficient evidence on an issue to raise it in a case.”

5.1.2 The specific considerations that apply to cyber operations

Joel Brenner has in his book America the Vulnerable: Inside the New Threat Matrix of Espionage, Crime, and warfare aptly explained that:

---

186 Nicaragua, para 60.
“The internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers to do your dirty work.” — 189

The identifying of whom is behind a cyber operation represent significant technical problems. This is also one of the reasons why it takes so much time to attribute a cyber operation to a state. This issue will be further discussed below.

In the cyber context, the state invoking self-defense against a cyber attack will have to demonstrate that: 190

a) The attack actually occurred,

b) That the attack raised to the threshold of a use of force or an armed attack, and that

c) The attack is attributable to a state or a non-state actor.

For the state to invoke the right to take countermeasures, however, it may be sufficient to prove that the cyber operation originated from a certain state, and that it did not exercise due diligence 191, without having to prove attribution to the state itself. 192 This may express proportionality between the severity of the attack and the burden of proof: a less serious incident will require a lower standard of proof of whether the attack occurred or not.

It should be emphasized that in the Nicaragua Case, the ICJ found that the situation that dominated the dispute was the secrecy and covert operations, which is also a typical characteristic of cyber operations. As information about conventional military operations usually will be classified, there is no reason to believe that this doesn’t apply to cyber operations as well. Furthermore, cyber operations will not be visible to the public before they reach step 7 of the kill chain, and therefore the operation is well protected from leaving visible traces before it is intended to.


One only need to look at the most famous cases of cyber operations against states allegedly launched by another states to realize how difficult the problem of evidence is in relation to cyber operations. Even though states like Russia, Israel and the United States have been confronted as launchers of cyber operations, all of them have rejected all accusations.

5.1.3 Attribution

One of the major challenges in the cyber context is to find out who the perpetrator is. In order to launch responses to a cyber operation, either countermeasures or self-defense, it is crucial to know who actually did it in the first place.

The rules of attribution for the purposes of state responsibility have been codified in the Part One of the Articles on the Responsibility of States for Internationally Wrongful Acts (Articles on State Responsibility, based on the existing customary law) adopted by the International Law Commission (ILC), as well as have been articulated in the cases of the ICJ. The drafters of the Tallinn Manual have based their sixth rule on the Articles on State Responsibility, which states that:

“A State bears international Legal Responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation.”

According to the Articles on State Responsibility, a state bear responsibility for an act when the act:

(a) is attributable to the State under international law; and

(b) constitutes a breach of an international obligation of the State.

Such a breach can consist of either an act or an omission. Roscini argues that there are three levels of evidence that are needed to attribute a cyber attack to a specific state:

194 The Tallinn Manual, p. 29.
196 Articles on State Responsibility Art. 2.
“First, the computer(s), or server(s) from which the operations originate must be located; secondly, it is the individual that is behind the operation that need to be identified; and thirdly, what needs to be proved is that the individual acted on the behalf of a state so that his or her conduct is attributable to it”.  

A method that complicates the attribution process even more is the use of foreign servers to launch the attack. For example, Stuxnet has been traced back to servers in Denmark and Indonesia. If an operation is launched this way, the victim state will only be able to attribute the attack to the state where the server is located, and have to depend on that state for help to find the origin of the attack. However, not all states will necessarily cooperate and provide the information requested by the victim state. For such cases, the Tallinn Manual has stated that the fact that a cyber operation has been routed via the cyber infrastructure of another state is not sufficient evidence for attributing the operation to that state. In this context, The Manual establishes a standard for behavior for states: states shall not knowingly allow the cyber infrastructure on its territory or under governmental control to be used for acts that unlawfully or adversely affect other states. The Manual builds these rules on the principle of sovereignty,

One can argue that the problem of attribution has to be seen in concert with the principle of necessity. Let's say, for example, that it takes six months to identify the perpetrator after an armed attack, and that it can be proved beyond reasonable doubt that he can be attributed to a state. Due to the high level of sophistication that is expected of future cyber operations, the identification process may prove to be comprehensive, difficult and take months. The problem that could arise then, is that after that time, is the act of self-defense still a necessary act, or is the right to self-defense lost on the way to the final attribution?

The same problem would rise regarding the scale and effects of an armed attack. How long is it required that a state must wait in order determine that the scale and effects sufficiently

---

200 The Tallinn Manual, p. 36.
fulfills the requirement of an armed attack? Say that a state is aware of a cyber operation interfering with national critical infrastructure, with the potential to cause massive injury to both property and persons.

The problem with the extension of existing rules and principles to new scenario like cyber operations is that they do not take into account their uniqueness and might prove to be too general.\textsuperscript{202} For instance, in accordance with the Westphalian order, existing rules of international law apply to and imply the existence of territory with geographical borders over which states exercise sovereignty or at least jurisdiction, while cyberspace is an apparently borderless, continuously developing man-made domain.\textsuperscript{203} However, it has been observed that:

"\textit{Components of cyberspace are not immune from territorial sovereignty nor from the exercise of State jurisdiction}".\textsuperscript{204}

In that context, it is important to remember that cyberspace consists of physical and syntactical layers.\textsuperscript{205} The former includes the physical infrastructure through which the data travels wired or wireless, including servers, routers, satellites and the computers, while the latter includes the protocols that allow data to be routed and understood, as well as the data and the software used.\textsuperscript{206} The Internet itself is nothing but a "\textit{set of inter-connected computer networks linked to state territory and, thus, is liable to the exercise of sovereign jurisdiction on a territorial basis}".\textsuperscript{207} This means that a cyber operation can be "territorialized" by focusing on the location of the cyber infrastructure used to conduct the operations and on where they occur.\textsuperscript{208}

5.1.3.1 The attribution of acts by non-state actors to a state

Article 8 on State Responsibility on conduct controlled by or directed by a state sounds:

“The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct.”

The Tallinn Manual emphasizes that this norm is especially relevant in the cyber context. They exemplify the situation where a private company on a contract with the state undertakes to conduct cyber operations against another state (cyber volunteers), or the state may trust the mission to a private person.

According to the commentary to the Articles, the most common example of such non-state actor attribution is where a state organ supplement their own activity by recruiting or instigating private persons or groups that act as so-called auxiliaries, meaning that they serve the organ, but remain outside or the organizational structure.

The criteria for state responsibility under article 8 are that the state has some degree of control over the operation carried out by the private company or person. This was stressed for the first time in the Nicaragua Judgment, where the ICJ articulated the effective control standard. The Court found that the alleged control over the contras by the United States was insufficient under the control standard, and emphasized that it could not be proved that the United States has such “effective control”. Only if such, the United States could be held legally responsible for the conduct.

5.2 Countermeasures

This section of the thesis seeks to clarify if a state has a right to respond to cyber operations that do not constitute an armed attack. As mentioned previously, an armed attack acted out by

---

209 Note that the three terms "instructions", "direction" and "control" are disjunctive; it is sufficient to establish any one of them. However, the "instructions", "direction" and "control" must be related to the conduct that is claimed to be an internationally wrongful act. Articles on State responsibility, Art 8, para 7.

210 The Tallinn Manual, p. 32.

211 The Tallinn Manual, p. 32.

212 Articles on State Responsibility, Art 8, para 7.

213 Nicaragua, para, 115.
a state could justify the use of self-defense in response by the victim state. Acts below the threshold of an armed attack, however, does not have a corresponding option for response, even though the hostile act could constitute a use of force. The Draft Articles on State Responsibility presents countermeasures as an option that injured states may seek to vindicate their rights and to restore the legal relationship with the state responsible for the wrongful act.\textsuperscript{214} Countermeasures consist of conduct inconsistent with a state’s international obligations on response to a prior violation of international law by another state.\textsuperscript{215}

The basis for the use of countermeasures is the separation of the concepts of armed reprisals and self-defense. In The Draft Articles the separation is reflected in two different articles, Article 21 (self-defense) and 22 (countermeasures). The Commission explained that:

"The term "countermeasures" covers that part of the subject of reprisals not associated with armed conflict."\textsuperscript{216}

The Tallinn Manual include cyber operations by stating in its 6\textsuperscript{th} rule that states bear the international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation. This rule is in accordance with international customary law, largely reflected in The Draft Articles on State Responsibility. Furthermore, the Manual states that a state injured by an international wrongful act may resort to proportionate countermeasures (including cyber countermeasures) against the responsible state.\textsuperscript{217}

According to the commentary of The Draft Articles on State Responsibility, countermeasures are

"measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order procure cessation and reparation".\textsuperscript{218}

\textsuperscript{214} Articles on State Responsibility, chapter II, para. 1.
\textsuperscript{216} Articles on State Responsibility, chapter II, para. 3.
\textsuperscript{217} The Tallinn Manual, p. 36.
\textsuperscript{218} Draft Articles on Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the work of its 53\textsuperscript{rd} session, UNGAOR, 56\textsuperscript{th} session, sup. No 10 (A/56/10), chapter IV.E.1, p. 128. Available at
In order for a victim state to resort to countermeasures, it must meet the conditions set in the relating law, and the act (in this context a cyber operation) cannot amount to an armed attack (or a use of force). In the *Case Concerning the Gabcikovo-Nagymaros Project*, the ICJ set out a three-part test justifying proportionate countermeasures.\(^{219}\)

First, the action must be taken in response to an internationally wrongful act of another state and must be directed against that state. Second, the victim state must have called upon the state committing the act to discontinue the wrongful conduct or to make reparation for it. Finally, the effect of the countermeasure must be proportionate with the injury suffered. In the case of countermeasures, the test of proportionality differs from self-defense where the test is related to the threat, rather than the harm suffered.\(^{220}\) In respect of a cyber operation this would seem to fit with current state practice, as most attacks to this date have merely result in states requesting the alleged perpetrator to cease their actions.\(^ {221}\) However, it should be noted that in the cases reported so far, the suspected perpetrator has denied any involvement with the attack.

Furthermore, the Court Stated in the case that the purpose of countermeasures is to induce the offending state to comply with its obligations under international law, and therefore, the measure must be reversible.\(^ {222}\) This is also in accordance with Article 49(1) of the Articles on State Responsibility.

One question is whether the state victim of a cyber attack can adopt countermeasures involving use of force against the attacker? Article 50 of the Articles on State Responsibility provides that countermeasures cannot amount to a use of force. However, this position was challenged by Judge Simma in the Oil Platform Case, where he argued that countermeasures could involve a limited degree of military force when in response to an act that itself was a use of force, but did not qualify as an armed attack.\(^ {223}\) Simma justified this position by

\(^{222}\) Articles on State Responsibility, chapter II, para. 87.
\(^{223}\) Oil Platform Case, dissenting opinion of Judge Simma, (6.nov), paras. 12-13.
suggesting a distinction between a full scale self-defense response under Article 51 and other hostile acts below the Article 51 threshold. This distinction would justify

"proportionate defensive measures on the part of the victim, equally short of the quality and quantity of actions in self-defense expressly reserved in the United Nations Charter".\textsuperscript{224}

The view was also favored by a minority of the drafters of the Tallinn Manual, but all agreed upon that countermeasure could not rise to the level of an armed attack.\textsuperscript{225} Dinniss argues that Simma’s treatment of the conditions in respect of forcible countermeasures is linked to the classic self-defense analysis, rather than the criteria for non-forcible countermeasures.\textsuperscript{226} The criteria will be explained below. As this view is one hold by a minority, it will only be addressed here.

\section*{5.3 Self-defense}

\subsection*{5.3.1 The UN Charter article 51}

According to article 51 of The UN Charter,

"[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations".

The drafters of The Charter did not intend to exclude self-defense entirely, but has restricted the scope considerably.\textsuperscript{227} In order to trigger the right to self-defense, the victim state must be the target of an armed attack.

In its 1996 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, the International Court of Justice said:

\begin{itemize}
  \item \textsuperscript{224} Oil Platform Case, dissenting opinion of Judge Simma, (6.nov), para. 12.
  \item \textsuperscript{225} The Tallinn Manual, p. 38.
  \item \textsuperscript{226} Dinniss (2012), p. 106.
\end{itemize}
"[T]he Court cannot lose sight of the fundamental right to every State to survival, and thus its right to resort to self-defense, in accordance with Article 51 of the Charter, when its survival is at stake."228

On the same page, the Court further explained ‘the very survival of a State would be at stake’ only in an extreme circumstance of self-defense’.229 These extreme cases of self-defense do arise from time to time, but Dinstein points out that the exercise of the right to self-defense is not limited to such catastrophic circumstances.230 The Court explains in the judgment that such extreme circumstances may justify the use of nuclear weapons.231

The essence of self-defense is self-help, which means that a state, under certain conditions set under international law, may respond to an unlawful force with lawful force.232 The self-help can be displayed in a variety of ways, such as the breaking of diplomatic relations or forcible measures.233 However, the self-help under article 51 is limited to a permissible form of ‘armed self-help’.234 Dinstein explains that legal scholars regard the two concepts as related yet separate.235

5.3.2 The right to self-defense in international customary law

In the following I will present the foundation of the right to self-defense in international customary law.

The traditional right to self-defense in international customary law arose from the Caroline case.236 The dispute revolved around an incident in 1837 in which British subjects seized and destroyed a vessel in an American port, The Caroline.237 The Caroline was destroyed because the ship had been supplying groups of American nationals, who had been conducting raids into Canadian territory.238 After the incident, the US Secretary of State laid down the essentials of self-defense in their correspondence with British authorities, stating that there

228 Advisory Opinion, para. 96.
229 Advisory Opinion, para. 97
231 Advisory Opinion, para. 97
233 Dinstein, (2012), p. 188.
234 Dinstein, (2012), p. 188.
235 Dinstein, (2012), p. 188.
had to exist "a necessity of-defense, instant, overwhelming, leaving no choice of means, and no moment for deliberation." The case has also laid down the basics for anticipatory self-defense, which is outside the scope of this paper.

The International Court of Justice stated in the Nicaragua Judgment that:

"The Court observes that the United Nations Charter, the convention to which most of the United States argument is directed, by no means cover the whole area of the regulation of the use of force in international relations".

and that Article 51

"does not contain any specific rule whereby self-defense would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in international customary law".

In the latter quote, the Court noted that the criteria of proportionality and necessity are not enshrined in Article 51 but formed a part of the customary right of self-defense. In addition to this, the Court clarified the problem of applying customary law where there was an overlapping rule found in a treaty. The United States argued in the case that the Court was precluded from applying any rule of international customary law which also was the subject of provision in the relevant multilateral treaties. In other words: there was no room for customary law if the customary rules and the Charter provisions where identical. The Court refused to follow this line of reasoning, and found that the incorporation of customary law into treaty law did not deprive it of its applicability as distinct from that of the treaty norm, "even if the rules would be completely identical." By saying this, the Court concluded that international customary law continues to exist and to apply, separately from international treaty law, even where the two sources of law have an identical content.

240 Nicaragua, para. 176.
241 Nicaragua, para. 176.
244 Nicaragua, para. 177.
245 Nicaragua, para. 179.
The Charter itself testifies to the existence of individual or collective self-defense as international customary law.\textsuperscript{246} On one essential point, the Charter itself refers to pre-existing law, by addressing the right to self-defense under article 51 as an "inherent right" (in the French text the "droit naturel") and “natural” right, and on this basis, found that the Article 51 only is meaningful when read in this context.\textsuperscript{247}

In The Principles of International Law Concerning Friendly Relations and Co-operations among States in accordance with the Charter of the United Nations, the reference to the prohibition of the use of force is followed by a paragraph stating that:

"Nothing in the foregoing paragraphs shall be constructed as enlarging or diminishing in any way the scope of these provisions of the Charter concerning cases in which the use of force is lawful".\textsuperscript{248}

In Nicaragua, ICJ based its decision on the norms of international customary law concerning the self-defense against an armed attack that has already occurred.\textsuperscript{249} ICJ stated in Nicaragua that the Declaration on Friendly Relations demonstrates that the members of the General Assembly regard the prohibition of use of force constituted by the right to self-defense as already being a matter of international customary law.\textsuperscript{250} According to the Court, the framers of the Charter thereby acknowledged that self-defense was a pre-existing right of a customary nature, which the drafters wanted to preserve.\textsuperscript{251}

Article 51 only addresses the Members of the United Nations, as subjects who can carry out self-defense, but since self-defense are a part of international customary law as well as the law of the Charter, it will therefore also apply to non-members of the United Nations.\textsuperscript{252}

\textsuperscript{246} Nicaragua, para.193.
\textsuperscript{247} Nicaragua, para. 176.
\textsuperscript{248} UN Doc A/RES/25/2625, Declaration of the Principles of International Law Concerning Friendly Relations and Co-operations among States in accordance with the Charter of the United Nations, 24 October 1970.
\textsuperscript{249} Dinstein, (2012) p. 196.
\textsuperscript{250} Nicaragua, para 193.
\textsuperscript{251} Nicaragua, para. 176.
5.3.3 The criteria for self-defense

The reaction in self-defense against cyber operations amounting to an armed attack, must meet the requirements of proportionality, necessity and immediacy.\(^{253}\) Even though Article 51 does not refer them, the 1996 Advisory Opinion on Nuclear Weapons stated that:

\[ \text{"The submission of the exercise of the right to self-defense to the conditions of necessity and proportionality is a rule of customary international law, but "this dual condition applies equally to Article 51 of the Charter, whatever the means of force employed."}^{254} \]

In the cyber context, the United States has reaffirmed that a use of force in self-defense against a cyber attack "must be limited to what is necessary to address an imminent or actual armed attack and must be proportionate to the threat that is faced."\(^{255}\)

It is important to note that the concepts of proportionality and necessity under the \textit{jus ad bellum} are distinct from the concept of military necessity and the rule of proportionality under \textit{jus in bello}. As these principles are closely connected, the different discussions below will contain elements of all, even though they are divided in separate sections.

5.3.3.1 The principle of proportionality

The condition of proportionality has been described as "\textit{the essence of self-defense}".\(^{256}\)

\[ \text{. The International Court of Justice has repeatedly confirmed that self-defense, individual or collective, warrants only those measures which are "proportional to the armed attack and necessary to respond to it, a rule well established in international customary law."}^{257} \] These principles are not stated in the UN Charter, but are often traced back to the Webster formulation in the Caroline incident, as cited above.

\(^{254}\) Advisory Opinion, para. 41.  
\(^{255}\) UN Doc A/66/152, 15 July 2011, p. 19.  
\(^{257}\) Nicaragua, paras. 176 and 194, Advisory Opinion, para. 41, Oil Platforms Case, para. 74, Armed Activities Case, para. 147.
In short, the principle of proportionality requires the weighting of the response against its permitted purpose of halting and repelling the attack, or in the case of anticipatory self-defense, preventing it from happening. This shows that the principle of proportionality must be applied with some degree of flexibility, meaning that this relative term will be acted out differently in all cases involving responses to an armed attack. In other words, the options for self-defense by State B are limited and contingent by the armed attack acted out by State A.

The problem with "calculating" proportionality in the cyber context resides in the speed and covert nature of cyber operations: it might be difficult to establish the magnitude and consequences. Furthermore, the calculation might prove to be difficult in advance because of the interconnectivity of information systems: as with biological weapons, malware sent through cyberspace might spread uncontrollably.

In short, proportionality in the cyber context is more than anything a technical issue: customized cyber reactions in self-defense are possible if the software is written with this purpose in mind, and requires a high degree of information on the targeted systems, which can be collected through traditional intelligence of cyber exploitation. Stuxnet is an excellent example of software designed to make the proportionality assessment difficult. It did little harm to computers and networks, contained safeguards to prevent each infected computer from spreading the worm to more than three other, in addition to being programmed to erase itself on 24 June 2012.

5.3.3.2 The principle of necessity

To fulfil the principle of necessity generally, "non-forcible remedies must either prove futile in limine or have in fact been exhausted in an unsatisfactory manner." This means that the final outcome is that there is no effective substitute for the use of force in self-defense.

---

258 Dinniss, p. 104.
The state must attribute the attack to a specific source, characterize the intent behind the attack, and conclude that the state must use force in response.\textsuperscript{265}

Necessity requires that a use of force, including cyber operations that amount to a use of force, is needed to successfully repel an imminent attack or one that is underway.\textsuperscript{266} However, this does not mean that force has to be the only way to respond. It merely requires that non-forcible measures be insufficient to address the situation. The forceful actions may be combined with non-forceful measures like economic sanctions, law enforcement or diplomacy.\textsuperscript{267}

According to the authors of The Tallinn Manual, the key to the necessity analysis in the cyber context is the existence, or lack, of alternative courses of action that do not rise to the level of use of force.\textsuperscript{268} Roscini clarifies that even a cyber attack that is severely disrupting the critical infrastructure of a state, does not automatically entitle the attacked state to use forcible measures in self-defense in all cases, as the use has to be proportional and necessary.\textsuperscript{269} For example, if a defensive cyber attack or a cyber attack below the use of force is reasonable means to react, a use of force in self-defense would be unnecessary and/or disproportionate and thus unlawful, even if the attacking cyber operation amounted to an armed force.\textsuperscript{270} Dinstein argues for a high threshold regarding when the victim state are affected by a disruptive computer network attack. He states that in a situation involving a computer network attack, an act of self-defense would be vindicated as an appropriate response only in "outré circumstances", such as a catastrophic event of a cyber attack-induced nuclear meltdown.\textsuperscript{271}

5.3.3.3 The principle of immediacy

The principle of immediacy indicates that the activation of self-defense counter-measures must not be too tardy.\textsuperscript{272} Yet, as Dinstein points out, the act of self-defense does not have to commence within minutes, or even days, from the original armed attack. The state under

\textsuperscript{266} The Tallinn Manual, p. 62.
\textsuperscript{267} The Tallinn Manual, p. 62.
\textsuperscript{268} The Tallinn Manual, p. 62.
\textsuperscript{269} Roscini, (2014), p. 75.
\textsuperscript{270} Roscini, (2014), p. 75.
\textsuperscript{271} Dinstein, (2002), p. 110.
\textsuperscript{272} Dinstein, (2002), p. 110.
attack must be given a reasonable time to respond, and it can’t be expected to shift from peace to war instantaneously. This led to the conclusion that immediacy does not mean "instantaneous", and allow some flexibility. Flexibility is required in the case of cyber attacks: if a state’s military computer system have been incapacitated by an attack, it might take some time for it to be able to react with either cyber or kinetic means. Furthermore, gathering of sufficient evidence in order to attribute the attack to a state, can be, as discussed above, a time-consuming task.

Textually, the Article 51 refers to a situation in which an "armed attack occurs". This will cover incidents in which the effects of the armed attack have already materialized, that is, when the cyber attack has caused, or is in the process of causing, damage or injury.

---

275 The Tallinn Manual, p. 63
6 Conclusions

As has been shown, as far as international law is concerned, cyber operations do not exist in a legal vacuum, but is subject to well established principles and rules. However, transposing these rules to a new domain raises a number of difficult questions.

As seen in this thesis, a cyber operation can constitute use of force and an armed attack, if the scale and effects of the attack causes death or injury to persons or damage property, or otherwise are comparable to the ones caused by kinetic weapons.

The constant comparison to kinetic weapons and operations can be helpful, but doesn’t quite catch the uniqueness of cyber operations, making the traditional concepts of attribution, self-defense and countermeasures hard to adapt.

The work with this thesis has shown that the questions discussed here, have been under the radar of states and scholars for many years, and it may seem like we are no further a solution today, compared to the discussion 10-15 years ago.

In order to clarify the legal principles and rules discussed in this paper, I think that we have to witness a cyber attack producing devastating effects before the legal realm can be adjusted. Only when a full scale attack occurs, it will be clear whether the current legal paradigm can cope with or not.
7 Table of reference

Books


Crawford, James, (2012), *Brownlie's Principles of Public International Law*, Oxford University Press


Riddell, Anna and Plant, Brendan, (2009), *Evidence before the International Court of Justice*. London: British Institute of International and Comparative Law


Sharp, Walter, (1999), *Cyberspace and the Use of Force*. Falls Church, Va.: Aegis Research Corp


**Articles**


Green, James, (2009), *Fluctuating Evidentiary Standards for Self-defense in the International Court of Justice*, International and Comparative Law Quarterly vol. 58


Henkin, Louis, (1971), *The Reports Of The Death of Article 2(4) are Greatly Exaggerated*, AJIL 65


Rid, Thomas, (2013), *Cyber War Will Not Take Place*, Journal of Strategic Studies, Vol. 35, Iss. 1


Schmitt, Michael, (2012). The "Use of Force" in Cyberspace: A Reply to Dr Ziolkowski. Available online: https://ccdcoe.org/publications/2012proceedings/5_4_Schmidt_ResponseToZiolkowski.pdf (last accessed on 8 March 2016)


Waldock, Claud Humphrey Meredith, The Regulation of the Use of Force by Individual States in International Law, Rec de Cours 81 (1952-II)


Newspapers and Magazines


**Treaties**

Charter of the United Nations, San Francisco, 26 June 1945, in force 24 October 1945. 1 UNTS XVI.


The Statute of the International Court of Justice

Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, A/RES/2625 (XXV) of 24 October 1970

Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, UN Doc. A/RES/42/22, 18 November 1987

**Judicial decisions**


*Case Concerning the Gabčíkovo-Nagymoros Project*, (1997), ICJ Reports 3, International Court of Justice


*Dispute Regarding Navigational and Related Rights* (Costa Rica v Nicaragua) Judgement, 13 July 2009, ICJ Reports 2009

*Case Concerning Oil Platforms*, (2003), (Iran v. United States), ICJ Rep. 161

*Case Concerning Armed Activities on the Territory of the Congo* (Congo v. Uganda), ICJ Rep. 168
UN Documents

Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, A/RES/42/22 of 18 November 1987.

Declaration of the Principles of International Law Concerning Friendly Relations and Co-operations among States in accordance with the Charter of the United Nations, 24 October 1970. UN Doc A/RES/25/2625

Competence of the General Assembly for the Admission of a State to the United Nations, ICJ Reports 1950


Security Council Resolution 1368 (12 September 2001) Threats to international peace and security caused by terrorist acts

Security Council Resolution 1373 (28 September 2001) Threats to international peace and security caused by terrorist acts


Other official documents


The Yearbook of the International Law Commission, Documents of the Fiftieth Session, Vol. 1

International Committee of the Red Cross, 31st International Conference of the Red Cross and Red Crescent, International Law and the Challenges of Contemporary Armed Conflicts, Report 31IC/11/5.1.2, October 2011

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013


